Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (currently amended) A method ~~for detecting and preventing security breaches in a network~~, ~~the method~~ comprising:

reassembling a plurality of TCP packets, in network traffic, into a TCP stream;

inspecting the TCP stream to detect information indicative of a security breach;

grouping the plurality of TCP packets into packet flows and communication sessions;

storing information regarding the packet flows in packet flow descriptors, where each of the packet flow descriptors points to one of the communication sessions and each of the communication sessions points to one or more of the packet flow descriptors ~~the packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type~~;

~~inspecting the TCP stream to detect information indicative of a security breach;~~

dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of the [[a]] security breach;

forwarding a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of the [[a]] security breach,

where ~~wherein~~ inspecting the TCP stream to detect information indicative of a security breach comprises:

storing a plurality of protocol specifications supported by the network in a protocol database,

querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database, and

searching for a network attack identifier, in the TCP stream, based on the packet flow descriptors and communication sessions associated with the TCP stream.

2. (currently amended) The method of claim 1, where ~~wherein~~ inspecting the TCP stream to detect information indicative of the security breach ~~breaches~~ comprises inspecting the TCP stream for protocol irregularities.

3. (currently amended) The method of claim 1, where ~~wherein~~ inspecting the TCP stream to detect information indicative of the [[a]] security breach comprises searching the TCP stream for attack signatures.

4. (currently amended) The method of claim 3, where ~~wherein~~ searching the TCP stream for attack signatures comprises using stateful signature detection.

5. (currently amended) The method of claim 1, where ~~wherein~~ inspecting the TCP stream to detect information indicative of the [[a]] security breach comprises using a plurality of network intrusion detection methods.

6. (currently amended) The method of claim 5, where ~~wherein~~ the plurality of network intrusion detection methods comprises at least protocol anomaly detection.

7. (currently amended) The method of claim 5, where ~~wherein~~ the plurality of network intrusion detection methods comprises at least signature detection.

8. (canceled)

9. (canceled)

10. (currently amended) The method of claim 1, further comprising searching the packet flow descriptors for traffic signatures.

11. (canceled)

12. (currently amended) The method of claim 1, where ~~wherein~~ the network attack identifier comprises a protocol irregularity.

13. (currently amended) The method of claim 1, where ~~wherein~~ the network attack identifier comprises an attack signature.

14. (canceled)

15. (currently amended) The method of claim 1 [[14]], where ~~wherein~~ the ~~plurality of~~ network attack identifier ~~identifiers~~ comprises at least a protocol irregularity.

16. (currently amended) The method of claim 1 [[14]], where ~~wherein~~ the plurality of network attack identifiers comprises at least an attack signature.

17. (currently amended) The method of claim 13, where ~~wherein~~ the attack signature and a plurality of traffic signatures are stored in a signatures database.

18. (currently amended) A method comprising:

reassembling a plurality of TCP packets into a TCP stream;

inspecting the TCP stream to detect information indicative of a security breach;

dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach;

forwarding a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of a security breach; and

grouping the plurality of TCP packets into packet flows and communication sessions, where ~~wherein~~ grouping the plurality of TCP packets into the packet flows and the communication sessions comprises:

storing information regarding the packet flows and the coomincation sessions in a hash table, where storing the information regarding the packet flows and the communication sessions in a hash table comprises:

~~wherein inspecting the TCP stream to detect information indicative of a security breach comprises:~~

storing information regarding the packet flows in packet flow descriptors, where each of the packet flow descriptors points to one of the communication sessions and each of the communication sessions points to a plurality of the packet flow descriptors; and

where inspecting the TCP stream to detect information indicative of the security breach further comprises:

searching for a network attack identifier, in the TCP stream, based on the packet flow descriptors and the communication sessions associated with the TCP stream~~, wherein storing the packet flows and~~

~~sessions in a hash table comprises computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type~~.

19. (canceled)

20. (canceled)

21. (currently amended) The method of claim 3, where ~~wherein~~ searching the TCP stream for attack signatures comprises:

querying a signatures database to identify ~~determine whether there are~~ matching attack signatures in the TCP stream.

22. (canceled)

23. (currently amended) The method of claim 1, further comprising:

reconstructing the plurality of TCP packets from a plurality of packet fragments.

24. (currently amended) A system ~~for detecting and preventing security breaches in network~~, ~~the system~~ comprising:

at least one sensor, implemented in hardware, where the at least one sensor is to:

reassemble a ~~TCP reassembly software module for reassembling~~ a plurality of TCP packets, in network traffic, into a TCP stream;

inspect ~~a software module for inspecting~~ the TCP stream to detect information indicative of a security breach;

drop ~~a software module for dropping~~ a TCP packet from the TCP stream if the TCP stream contains information indicative of the [[a]] security breach;

forward ~~a software module for forwarding~~ a TCP packet, from the TCP stream, to a network destination if the TCP stream does not contain information indicative of the [[a]] security breach, ~~; and~~

where the at least one sensor further is to:

store a plurality of protocol specifications supported by the network in a protocol database,

query the protocol database to determine whether the plurality of TCP packets is compliant with one or more of the plurality of protocol specifications in the protocol database,

group the plurality of TCP packets into packet flows and communication sessions, and

store information regarding the packet flows in packet flow descriptors, where each of the packet flow descriptors points to one of the communication sessions and each of the communications session points to one or more of the packet flow descriptors,

where, when inspecting the TCP stream, the at least one sensor further is to search for a network attack identifier, in the TCP stream, based

on the packet flow descriptors and the communication sessions associated with the TCP stream

~~at least one processing device configured to execute the TCP reassembly software module, the software module for inspecting the TCP stream, the software module for dropping a TCP packet and the software module for forwarding a TCP packet,~~

~~wherein the software module for inspecting the TCP stream comprises at least a protocol anomaly detection software module and a flow manager software module, the protocol anomaly detection software module comprising:~~

~~a routine for storing a plurality of protocol specifications supported by the network in a protocol database, and~~

~~a routine for querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database,~~

~~wherein the flow manager software module is configured to:~~

~~group the plurality of TCP packets into packet flows and sessions,~~

~~store the packet flows in packet flow descriptors, the packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type, and~~

~~search for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream.~~

25. (currently amended) The system of claim 24, where the at least one sensor further is to:

reconstruct ~~further comprising an IP defragmentation software module for reconstructing~~ a plurality of packet fragments into the plurality of TCP packets.

26. (canceled)

27. (currently amended) A system, comprising:

a TCP reassembly software module to reassemble ~~for reassembling~~ a plurality of TCP packets, in network traffic, into a TCP stream;

a software module to inspect ~~for inspecting~~ the TCP stream to detect information indicative of a security breach;

a software module to drop ~~for dropping~~ a TCP packet, from the TCP stream, if the TCP stream contains information indicative of the [[a]] security breach;

a software module to forward ~~for forwarding~~ a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of the [[a]] security breach;

a flow manager software module to group ~~for grouping~~ the plurality of TCP packets into packet flows and communication sessions, where ~~wherein~~ the flow manager software module further is to: ~~comprises~~

~~a routine~~ store information regarding ~~for storing~~ the packet flows and the communication sessions into a hash table, where, when the flow manager software module is to store the information regarding the packet flows and the communication sessions into the hash table, the flow manager software module further is to:

store information regarding ~~storing~~ the packet flows in packet flow descriptors, where each of the packet flow descriptors points to one of the communication sessions and each of the communication sessions points to a plurality the packet flow descriptors; and

where the software module to inspect the TCP stream further is to search ~~searching~~ for a network attack identifier, in the TCP stream, based on the packet flow descriptors and the communication sessions associated with the TCP stream~~; and~~

~~at least one processing device configured to execute the TCP reassembly software module, the software module for inspecting the TCP stream, the software module for dropping a TCP packet, a software module for forwarding a TCP packet and the flow manager software module,~~

~~wherein the routine for storing the packet flows and sessions into a hash table comprises a routine for computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type~~.

28-30. (canceled)

31. (currently amended) The system of claim 24, where ~~wherein~~ the at least one sensor further is to:

~~software module for inspecting the TCP stream to~~ detect information indicative of the [[a]] security breach based on ~~comprises~~ a stateful signature ~~detection software module~~.

32. (currently amended) The system of claim 27, further comprising:

a traffic signature detection software module to search ~~for searching~~ the packet flow descriptors for traffic signatures.

33-36. (canceled)

37. (currently amended) The system of claim 24, where ~~wherein~~ the protocol specifications comprise specifications of one or more of:

a TCP protocol; an HTTP protocol; a SMTP protocol; a FTP protocol; a NETBIOS protocol; an IMAP protocol; a POP3 protocol; a TELNET protocol; an IRC protocol; a RSH protocol; a REXEC protocol; or a ~~and~~ RCMD protocol.

38. (currently amended) The system of claim 24 [[35]], where ~~wherein~~ the at least one sensor further is to:

query ~~stateful signature detection software module comprises a routine for querying~~ a signatures database to determine whether there are matching attack signatures in the TCP stream.

39. (canceled)

40. (currently amended) The system of claim 24, further comprising:

at least one processor to:

collect ~~a routine for collecting~~ a plurality of security logs and alarms recording information about security breaches found in the TCP stream;

store ~~a routine for storing~~ a network security policy identifying the network traffic to inspect and a plurality of network attacks to be detected and prevented;

distribute ~~a routine for distributing~~ the network security policy to one or more gateway points in the network; and

update [[a]] routine for updating the protocol database and a signatures database.

41. (currently amended) The system of claim 24, further comprising a graphical user interface to ~~comprising~~:

display ~~a routine for displaying~~ network security information to network security administrators; and

a routine for specifying a network security policy.

42. (currently amended) A system for detecting and preventing security breaches in a network, the system comprising:

a network intrusion detection and prevention sensor, located in a network gateway, where ~~wherein~~ the network intrusion detection and prevention sensor is ~~including at least one processor configured~~ to ~~execute~~:

reassemble ~~a routine for reassembling~~ a plurality of TCP packets into a TCP stream;

inspect ~~a software module for inspecting~~ the TCP stream to detect information indicative of a security breach, where, when the network intrusion and detection sensor is to inspect the TCP stream, the network intrusion and detection sensor further is to ~~wherein inspecting the TCP stream to detect information indicative of a security breach comprises~~:

store ~~storing~~ a plurality of protocol specifications, supported by a ~~the~~ network, in a protocol database, and

query ~~querying~~ the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database;

drop ~~a software module for dropping~~ a TCP packet from the TCP stream if the TCP stream contains information indicative of the [[a]] security breach; and

forward ~~a software module for forwarding~~ a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of the [[a]] security breach;

a central management server to control the network intrusion detection and prevention sensor; and

a graphical user interface to configure ~~for configuring~~ the network intrusion detection and prevention sensor,

where ~~wherein~~ the network intrusion detection and prevention sensor further is ~~comprises a flow manager software module and a traffic signature detection module, the flow manager software module being configured~~ to:

group the plurality of TCP packets into packet flows and communication sessions, ~~and~~

store information regarding the packet flows in packet flow descriptors, where each of the packet flow descriptors points to one of the communication sessions and each of the communication sessions points to one or more of the packet flow descriptors ~~the packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type~~, and

~~the traffic signature detection module is configured to:~~

search for a network attack identifier, in the TCP stream, based on the packet flow descriptors and the communication sessions associated with the TCP stream.

43. (currently amended) The system of claim 42, where ~~wherein~~ the network intrusion detection and prevention sensor is located within a firewall.

44. (currently amended) The system of claim 42, where ~~wherein~~ the network intrusion detection and prevention sensor is located outside a firewall.

45. (currently amended) The system of claim 42, where ~~wherein~~ the network intrusion detection and prevention sensor further is to: ~~comprises~~

reconstruct ~~an IP defragmentation software module for reconstructing~~ a plurality of packet fragments into the plurality of TCP packets.

46-54. (canceled)

55. (currently amended) The system of claim 42, where ~~wherein~~ the central management server further is to ~~comprises~~:

collect ~~a routine for collecting~~ a plurality of security logs and alarms recording information about the security breach ~~breaches~~ found in the TCP stream;

store ~~a routine for storing~~ a network security policy identifying the network traffic to inspect and a plurality of network attacks to be detected and prevented; and

distribute ~~a routine for distributing~~ the network security policy to the network intrusion detection and prevention sensor.

56. (currently amended) The system of claim 42, where ~~wherein~~ the graphical user interface further is to ~~comprises~~:

display ~~a routine for displaying~~ network security information to network security administrators;

display ~~a routine for displaying~~ status information regarding [[on]] the network intrusion detection and prevention sensor; and

specify ~~a routine for specifying~~ a network security policy.

57. (currently amended) A network intrusion detection and prevention sensor for detecting and preventing network security breaches at a network gateway, the network intrusion detection and prevention sensor comprising:

a flow manager software module to group ~~for grouping~~ a plurality of packets into packet flows and sessions;

a TCP reassembly software module to reassemble ~~for reassembling~~ ~~for reassembling~~ a plurality of TCP packets, from the plurality of packets, into a TCP stream;

a software module to inspect ~~for inspecting~~ ~~for inspecting~~ the TCP stream, based on ~~according to~~ the packet flows and the sessions, to detect information indicative of a security breach, where ~~wherein~~ inspecting the TCP

stream to detect information indicative of the [[a]] security breach comprises:

storing a plurality of protocol specifications, supported by a ~~the~~ network, in a protocol database, and

querying the protocol database to determine whether the plurality of TCP packets is ~~are~~ compliant with one or more of the plurality of protocol specifications in the protocol database;

a software module to drop ~~for dropping~~ a packet, from the plurality of packets, if the TCP stream contains information indicative of the [[a]] security breach;

a software module to forward ~~for forwarding~~ a packet, from the plurality of packets, to a network destination if the TCP stream does not contain information indicative of the [[a]] security breach;

a software module to:

group ~~for grouping~~ the plurality of TCP packets into packet flows and sessions, and

store information regarding ~~storing~~ the packet flows in packet flow descriptors, where each of the packet flow descriptors points to one of the sessions and each of the sessions points to one or more of the packet flow descriptors ~~the packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type~~; and

a software module to search ~~for searching~~ for a network attack identifier, in the TCP stream, based on the packet flow descriptors and sessions associated with the TCP stream~~; and~~

~~at least one processing device configured to execute the flow manager software module, the TCP reassembly software module, the software module for inspecting the TCP stream, the software module for dropping a packet, a software module for forwarding a packet, a software module for grouping the plurality of TCP packets and the software module for searching for a network attack identifier~~.

58. (currently amended) The network intrusion detection and prevention sensor of claim 57, further comprising:

an IP defragmentation software module to reconstruct ~~for reconstructing~~ a plurality of packet fragments into the plurality of TCP packets.

59. (canceled)

60. (currently amended) The network intrusion detection and prevention sensor of claim 57, where ~~wherein~~ the network intrusion detection and prevention sensor is controlled by a network security policy specifying ~~the~~ network traffic to inspect and a plurality of network attacks to be detected and prevented.

61. (currently amended) The network intrusion detection and prevention sensor of claim 60, where ~~wherein~~ the network security policy is defined by a network security administrator using a graphical user interface associated with the network intrusion detection and prevention sensor.

62. (currently amended) The network intrusion detection and prevention sensor of claim 61, where ~~wherein~~ the graphical user interface is to:

display ~~a routine for displaying~~ network security information to network security administrators;

display ~~a routine for displaying~~ status information regarding [[on]] the network intrusion detection and prevention sensor; and

specify ~~a routine for specifying~~ the network security policy.

63. (currently amended) The network intrusion detection and prevention sensor of claim 60, where ~~wherein~~ the security policy is stored by and distributed to the network intrusion detection and prevention sensor by a central management server.

64. (canceled)

65. (currently amended) The network intrusion detection and prevention sensor of claim 57, where ~~wherein~~ the software module to inspect

~~for inspecting~~ the TCP stream according to the packet flows and the sessions ~~to detect information indicative of a security breach~~ further comprises:

a protocol anomaly detection software module.

66. (currently amended) The network intrusion detection and prevention sensor of claim 57, where ~~wherein~~ the software module to inspect ~~for inspecting~~ the TCP stream based on ~~according to~~ the packet flows and the sessions ~~to detect information indicative of a security breach~~ further comprises:

a stateful signature detection software module.

67-69. (canceled)